

DEPARTMENT OF STATE
FISCAL YEAR 2008
PRIVACY IMPACT ASSESSMENT

**THE OFFICE OF FOREIGN MISSION INFORMATION SYSTEM
(TOMIS)**

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy Office
E-mail: pia@state.gov

The Department of the State

FY 2007 Privacy Impact Assessment for IT Projects

Introduction

Section 208 of the E-Government Act requires that agencies now conduct a Privacy Impact Assessment (PIA) for all new and significantly modified Information Technology (IT) projects. This includes projects that are requesting funding from the Office of Management and Budget (OMB), non-major systems requesting funding internally and those undergoing DOS IT Security Certification and Accreditation (C&A) process. The Privacy Impact Assessment (PIA) is an analysis of how information is handled:

- to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system;
- to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The PIA will help DOS employees consider and evaluate whether existing statutory requirements and key information management concepts are being applied to new and modified systems that contain personally information about members of the public. OMB, which has oversight of all federal agency implementation of the Privacy Act of 1974, as amended, will be particularly scrutinizing IT project budget requests on the Exhibit 300 based on the PIA in addition to the other requirements that are already in place. The score obtained on the PIA among other criteria will determine the funding of the IT project. IT projects scoring poorly on the PIA will be at risk of not being funded by OMB. The same scrutiny will be applied to non-major funding requests as well as systems undergoing the C&A process. Consequently, it is imperative that the attached PIA be fully **completed, certified and submitted** as indicated below.

The Office of Information Programs and Services (IPS) is responsible for conducting the PIA as part of its Department-wide implementation of the Privacy Act. The PIA will be reviewed and scored by IPS and will be provided with the Exhibit 300 to OMB. This score will reflect how well your system protects personal information and will be integrated with the score for security. This combined score will then be incorporated in your Exhibit 300 submission to OMB. The document will also be provided to the Office of Information Assurance for purposes of C&A. For non-majors, IPS will retain PIAs on file for future needs. A guide and a handbook are being provided along with the PIA questionnaire. Please refer to the PIA handbook while completing the questionnaire. For more detailed information you may refer to the guide. In addition, this Office will assist you in completing the PIA questionnaire should you have any questions not covered in the guide.

Department of State FY 2008 Privacy Impact Assessment

Once completed copies of the PIA may be provided to the following:

- Bureau/office IT Security Manager (when a C&A is required);
- Office of Information Programs and Services (A/RPS/IPS) Privacy Act Program Staff must be provided a copy of the PIA in all cases;
- Office of Management and Budget (OMB) Capital Planning Exhibit 300 Submission (when an Exhibit 300 is required).

Also please complete the certification page at the end of this document. Please note that you will receive a low score if all appropriate questions are not adequately answered and/or if the certification page is not completed fully. A guide and handbook are provided along with the PIA questionnaire. **You must refer to the handbook as you complete the PIA. The handbook mirrors each section of the PIA and provides instructions for each question.** For more detailed information, please refer to the guide.

A. CONTACT INFORMATION:

Who is the Agency Privacy Coordinator who is conducting this assessment?

**Ms. Charlene Thomas
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy**

B. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION:

- 1) Does this system collect, maintain or disseminate personally identifiable information about individual members of the public**?**

YES X NO__

Personally Identifiable Information (PII) is information about an identifiable individual that may include but is not limited to:

- o Information relating to race, national or ethnic origin, religion, age, marital or family status;
- o Information relating to education, medical, psychiatric, psychological, criminal, financial, or employment history;
- o Any identifying number, symbol or other particular assigned to the individual; and
- o Name, address, telephone number, fingerprints, blood type, or DNA.

An individual member of the public means, any person not acting in his/her official capacity as a federal government employee/contractor. This definition may include but no limited to:

- U.S. citizens whether natural born or naturalized;
- Legal Permanent Resident Aliens (LPRs);
- Aliens; and
- Federal Government Employees/Contractors acting solely in his/her own personal capacity.

System of Record, a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol or identifying assigned.

**** “Personally identifiable information from/about individual members of the public” means personally identifiable information from/about “any person not acting in his/her official capacity as a federal government employee/contractor”.**

If answer is yes, please complete the survey in its entirety.

If answer is no, please complete the certification page and submit the completed PIA to both of the following e-mail addresses: PIA@state.gov

2) Does a Privacy Act system of records already exist?

YES X NO

If yes, please provide the following:

System Name Diplomatic Security Records Number STATE-36

*“A new System of Records Notice (SORN) is **not** necessary.”*

If no, a Privacy system of records description will need to be created for this data.

3) What is the purpose of the system/application?

The Office of Foreign Missions Information System (TOMIS) application is a system used to determine and establish immunity and privileges for the Foreign Diplomatic Community in the United States. Privileges include vehicle registration, driver licenses, sale, gasoline and utility exemption and diplomatic immunity cards.

4) What legal authority authorizes the purchase or development of this system/application?

The legal authorities as documented in STATE-36, Diplomatic Security Records.

C. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system?

The categories of individuals that are covered by the system are documented in STATE-36, Diplomatic Security Records

2) What are the sources of the information in the system?

a. Who/what is the source of the information?

The source of the information is the individual or law enforcement agency(ies).

b. What type of information is collected from the source of the information?

The Office of Foreign Missions Information System (TOMIS) application is a system used to determine and establish immunity and privileges for the Foreign Diplomatic Community in the United States. Privileges include vehicle registration, driver licenses, sale, gasoline and utility exemption and diplomatic immunity cards; specific to capturing the following data items:

- Diver License data:
 - Name
 - Driver License Number
 - Date of birth, and
 - Citizenship
- Work History

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

The agency or source providing the information is responsible for verifying accuracy, in this case it is the Bureau of Diplomatic Security (DS).

b. How will data be checked for completeness?

Completeness of data will be checked through investigations and/or through personal interviews of the source(s) of the information.

- c. **Is the data current?** What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Investigations and/or through personal interviews will confirm whether data is current.

D. INTENDED USE OF THE DATA:

- 1) **Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?**

The Office of Foreign Missions Information System (TOMIS) application is a system used to determine and establish immunity and privileges for the Foreign Diplomatic Community in the United States. Privileges include vehicle registration, driver licenses, sale, gasoline and utility exemption and diplomatic immunity Cards; specific to capturing the following data items:

- Diver License data:
 - Name
 - Driver License Number
 - Date of birth, and
 - Citizenship.
- Work History

- 2) **Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?**

Yes. An aggregation of data from other federal agencies will be gathered to provide a complete picture of the diplomat and his family members to insure that neither the diplomat nor his family members are threats to the security of the United States or its citizens. This data includes the collection of information pertaining to criminal activities and abuse of privileges.

- 3) **Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?**

Yes. The information will assist in the determination whether to allow members of the Diplomatic Community with inappropriate behavior to remain in the United States.

- 4) **Will the new data be placed in the individual's record?**

Yes. The information will be added to the biographical information maintained on the individual.

5) How will the new data be verified for relevance and accuracy?

Verification will be made through investigations and/or personal interviews.

6) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

The identification of data pertaining to an individual is retrieved by the use of a personal identifying number (PIN) assigned by the system.

7) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Various reports are provided by the system for statistical, law enforcement, and management purposes. These reports are used by Department of State personnel and are Sensitive but Unclassified (SBU) and not for release outside of the Department without prior approval.

E. MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

TOMIS is operated at State Annex-20 (SA-20).

2) What are the retention periods of data in this system?

The retention period of data is consistent with established Department of State policies and Guidelines as documented in the Department's Disposition Schedule of Diplomatic Security Records, Chapter 11.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

The retention period of data is consistent with established Department of State policies and Guidelines as documented in the Department's Disposition Schedule of Diplomatic Security Records, Chapter 11.

4) Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

- 5) **How does the use of this technology affect public/employee privacy and does it restrict access to the system?**

No additional or new effect to privacy. Yes, access restrictions are in place.

- 6) **If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**

No, the system does not provide the capability to identify, locate, and monitor individuals.

- 7) **If the system is being modified, will the Privacy Act system of records Notice require amendment or revision? Explain.**

N/A: The system/application will not be modified to the degree whereby a new system of records notice (SORN) is required. The current system of records is sufficient.

- 8) **Are there forms associated with the system? YES ___ NO X**

If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

F. ACCESS TO DATA:

- 1) Who will have access to the data in the system?** *(e.g., contractors, users, managers, system administrators, developers, other)*

Access to the data in the system is on “a need-to-know” basis and/or under routine use criteria as explained in STATE-36.

- 2) What are the criteria for gaining access to the system?** *Are criteria, procedures, controls, and responsibilities regarding access documented?*

A criterion for gaining access to the system is based on “a need-to-know” basis. Criteria, procedures, controls, and responsibilities regarding access are all documented.

- 3) Will users have access to all data on the system or will the user’s access be restricted? Explain.**

Access will be restricted on “a need to know basis” specific to work related responsibilities.

- 4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access?** *(Please list processes and training materials)*

TOMIS provides a means of limiting access to areas within the application based on user ID, password, and “a need-to-know.” Moreover, the Bureau of Diplomatic Security employees and contractors must follow the System Behavior Rules established by the Department.

- 5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? YES**

If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? **YES**

Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended? **YES**

- 6) **Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

No

- 7) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?**

Other agencies will not have direct access to the data but the data may be shared with an agency upon request from the agency if that agency is listed as a routine user in STATE-36. The use of the data by the other agency will be restricted to the same purpose for which the data was originally collected.

- 8) **Who is responsible for assuring proper use of the SHARED data?**

The agency receiving the information is responsible for adhering to lawful restrictions.

ADDITIONAL COMMENTS: (optional)

None.